April 2004

Intelligent Vulnerability Monitoring

Protection through Continuous Surveillance

Table of Contents

Intelligent Vulnerability Monitoring – Protection through Continuous Surveillance

Executive Summary

Management of network security requires a layered approach where each layer is vital to the security and integrity of the institution, company or business. Each layer is responsible for protection from a defined set of threats. The sum of all layers far exceeds the protection from any single layer. This paper examines the threats caused by software vulnerabilities inherent in computers, servers and devices. In addition, this paper presents Catbird Networks' continuous Intelligent Vulnerability Monitoring (IVM) as a solution for around-the-clock protection.

A study conducted by the Computer Security Institute (CSI) and the FBI found for the fourth year in a row that the most frequent point of attack on systems is from the Internet. Hackers attempt to take advantage of these exposed systems by entering through vulnerable software holes where known weaknesses can be exploited. Any business connected to the Internet must protect their computers and information with effective vulnerability assessment programs. These programs encompass external assessments conducted from outside the firewall, and they also include internal assessments conducted within the protected network. Historically, companies conducted these assessments at periodic intervals – typically annually or quarterly. The problem is that new vulnerabilities are being discovered at the rate of over 300 per month, making these periodic scans ineffective against this growing threat.

According to the Computer Emergency Response Team (CERT), the majority of network intrusions occurred as a result of unpatched computers exposed to known vulnerabilities. The lack of proactive management of vulnerability threats, coupled with exposed systems, has caused billions of dollars in damages.

A company can protect its systems from attack if they are diligent in their efforts to stay informed, but it is next to impossible to accomplish this task manually. Moreover, conducting more frequent vulnerability assessments can be cost-prohibitive and the information provided can be next to impossible to digest.

Catbird Networks offers a solution to the growing vulnerability security problems – Intelligent Vulnerability Monitoring. Catbird's IVM provides constant surveillance of a customer's network to protect against new vulnerabilities that can threaten the network. Businesses depend on constant surveillance from anti-virus programs, and do not run these programs on periodic intervals because virus exposure can happen at any time. The same idea applies to vulnerability exposure, and with IVM, Catbird has the constant surveillance solution.

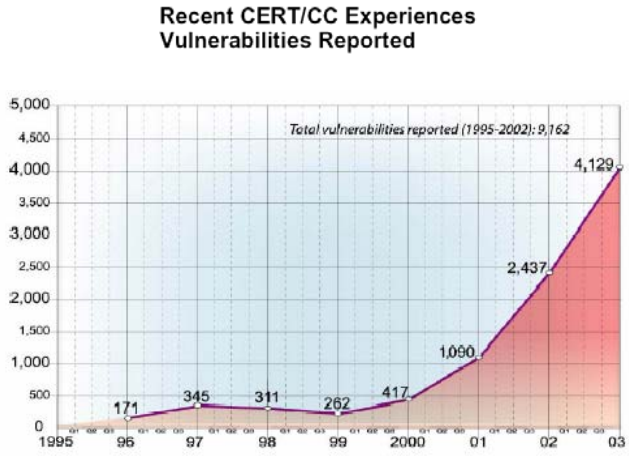
What are the causes of vulnerability exposures?

Businesses protect their networks and proprietary information through the deployment and management of a firewall, or series of firewalls. Authorized communication with the outside world is then accomplished through openings, or ports, in the firewall. An open port presents a potential vulnerability exposure; it offers hackers the opportunity to gain access to the network, the connected computers or systems, and the proprietary information being protected.

The computers protected behind the firewall can also be a point of vulnerability exploitation. Hackers know that the firewall is typically hardened, and that all internal PC's have outbound access. If an internal PC connects to a compromised web site, the hacker now has a path to directly exploit an unpatched vulnerability.

Most vulnerability exposures are the result of one of the following:

- **Unpatched systems.** When software vendors discover an error in their software, they will release a patch or a fix for the error. However, many companies fail to update their software with these patches to protect from these known vulnerabilities, enabling hackers to gain access and possibly control of the server or network.
- **Human error.** Networks are exposed due to simple human error. A port is left open, a configuration mistake is made, or a software upgrade causes other problems that go undetected until it is too late.



New vulnerabilities are currently being reported at a rate of over 300 per month.

Vulnerabilities threaten networks directly – and it is expected to get worse

Vulnerabilities are exploited through the rapid spread of worms and viruses; sometimes both are bundled under the description of malicious code. The malicious code will affix itself to other programs while replicating itself to exploit additional computers.

Prior to 2003, most malicious code was in the form of viruses, spread through email. These email-born viruses mass-mail themselves to every address in an infected computer's address book. Today, most enterprises have antivirus software installed to block these email messages and strip out the harmful executable file before it gets to the destination, eliminating its ability to be mistakenly opened and spread further.

In 2003, a major change in the type of malicious code reaping havoc on enterprises was witnessed. Malicious code directly attacked computers attached to a network without the need to be propagated via email. These attacks, called "perimeter attacks," require no interaction with a computer user to release their destructive payload. The spread of the attack is completely automatic. Experts agree that this trend is expected to continue in 2004.[1] Perimeter attacks represent potentially the largest threat to enterprises in the coming years.

Vulnerabilities are spreading faster than ever before

Two of the largest cyber attacks from 2003, Slammer and Blaster, were both perimeter attacks. In addition to attacking networks directly, they did so at speeds that warrant great concern. There are two components of this speed that further heighten the concern of network administrators:

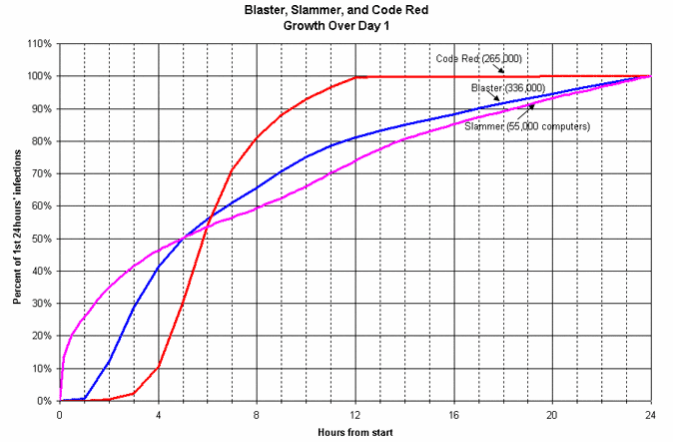
- The first component of speed is the timeframe between the publication of a known vulnerability and its exploitation.
- The second component of speed is rate at which these exploitations spread once the attack is initiated.

The Slammer attack started about six months after the first vulnerability advisory was published. In January of 2003, it proceeded to infect over 55,000 machines in the first day of the attack. In August of 2003, the Blaster attack was initiated only one month after the first vulnerability advisory was published, and it proceeded to infect over 100,000 machines in the first three-to-five hours of the attack.[2]

In some cases, the spread was due to an unpatched computer exposed through an open port in the firewall. In other cases, computers in networks, thought to be protected by a hardened firewall, were infected. This was the case in January at a nuclear power plant in Ohio. A contractor established an unprotected high-speed connection to the corporate network that allowed the infection to spread internally. It is imperative to have both internal and external vulnerability protection.

Although many attacks are spread via Microsoft software, the problem is not limited to just Microsoft. 2003 saw the development of vulnerability exploit code within a week of Cisco

announcing a major vulnerability within its router software. These routers manage the majority of Internet traffic.[3]



The Slammer and Blaster worm perimeter attacks are plotted against the Code Red email virus attack. The Code Red attack required the opening of an email message to release its destructive payload, where the Slammer and Blaster perimeter attacks required no human interaction to attack networks directly.

The speed of future attacks is expected to increase, making it more and more difficult to protect the enterprise. Experts now discuss the threat of "zero-day" attacks, where the exploitation of the vulnerability happens in conjunction with initial publication.

No end is in sight for the increase in new vulnerabilities

No matter which set of IT security indices you analyze, the cyber-threat due to vulnerabilities is increasing. Currently, there are over 300 new vulnerabilities being reported every month. The table below from CERT/CC depicts the increase in vulnerabilities reported since 1995. The CERT® Coordination Center (CERT/CC) specializes in Internet security, and is located at the Software Engineering Institute (http://www.sei.cmu.edu), a federally funded research and development center operated by Carnegie Mellon University (http://www.cmu.edu).

Vulnerabilities reported

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2003

Year	2000	2001	2002	2003
Vulnerabilities	1,090	2,437	4,129	3,784

Total vulnerabilities reported (1995-3Q 2003): **12,144**

Experts do not see an end to the trend of the quantity of new vulnerabilities drastically increasing in 2004.

Honest activities can expose networks to vulnerabilities

The second most frequent cause of vulnerability intrusions is from exploitation of configuration errors. CERT estimates that 24.6% of all intrusions are the result of these errors. Some of the primary causes of configuration errors include:

- Software upgrades
- Addition of new services
- New user authorizations
- Simple human errors

Because a firewall has over 64,000 ports, or potential points of entry, a port that is locked down today may not be secure tomorrow.

A periodic vulnerability assessment will typically catch these types of errors. The problem for most firms is that the assessments are not performed in a timely manner. The timeframe from the error to the assessment can be excessive, taking months to correct. The result: firms are now far in excess of the exploit cycle of the most recent major vulnerabilities.

Regulated industries have specific requirements to manage risk exposure to vulnerabilities

For regulated industries—such as financial institutions, health care, energy providers and public corporations—vulnerability management is no longer simply a best practices requirement, it is a regulatory requirement.

As stated in the beginning of this paper, security best practices require a layered approach. Monitoring for vulnerabilities is one of those layers, and therefore an important component of regulatory compliance. This compliance should be viewed as an ongoing process that is designed to identify, measure, manage, and control risks, including those due to vulnerabilities. Monitoring can be described as the continuous process of gathering and analyzing information in relationship to vulnerabilities that threaten the integrity, confidentiality, and security of information systems. This is true for all industries.

The Federal Financial Institution Exam Council (FFIEC) has provided guidance to financial institutions regarding security and monitoring for vulnerabilities:

> "A strong security program reduces levels of reputation and strategic risk by limiting the institution's vulnerability to intrusion attempts and maintaining customer confidence and trust in the institution."
>
> FFIEC IS Handbook, December 2002

The FFIEC also states that "strategies should consider the layering of controls."

The Gramm-Leach-Bliley Act of 1999 (GLBA) directs the financial industry to safeguard customer information. The act mandates that federal agencies develop standards for safeguarding customers' personal non-public information. These agencies have since dictated the management and control of vulnerability risks as a vital part of ensuring the confidentiality and integrity of customer information as well as the institution's financial information. Monitoring of systems and procedures is recommended to ensure that established controls are in place and functioning properly; it is also advised to prevent and detect vulnerabilities and actual or attempted attacks into systems. Federal banking regulators have issued guidance concerning the implementation of software patch management programs. To effectively provide such a program, an institution must monitor its systems for vulnerabilities.

While GLBA specifically addresses the regulated requirements for the financial industry, the Sarbanes Oxley Act of 2002 (SOX) addresses all publicly traded companies. SOX was created by Congress in an effort to restore investor confidence and improve corporate governance and transparency. Sections 302 and 304 of SOX require companies to establish, maintain, and report internal controls. Section 404 requires the annual reporting on the effectiveness of the internal control structure and integrity of financial information reporting. Information system controls are a critical element to internal controls and ensuring the integrity of financial information. Security monitoring, which includes monitoring for vulnerabilities, is an essential part of these overall information system controls.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires health care providers to identify vulnerabilities to its electronic protected health information (PHI) and to implement safeguards and countermeasures to mitigate the threats. Online access to PHI including bill payment information heightens the need for implementation of a vulnerability management program to monitor for vulnerabilities. The timely identification and implementation of a vulnerability management program is stressed as an essential part of complying with the HIPAA security regulations.

Energy providers are not exempt from implementing appropriate vulnerability controls. The North America Electric Reliability Council (NERC) has issued security guidance for power companies, which also include monitoring for vulnerabilities and implementing software patch management programs. In August of 2003, NERC adopted the Urgent Action Cyber Security Standard (UACSS). This standard requires each utility to implement a cyber security program to protect critical cyber assets related to the reliable operation of the bulk electric systems. This Urgent Action has since been replaced by a permanent standard for cyber security, where again, a critical component of the standard is the management of vulnerability risks.

Old school snapshots are not sufficient

Most Internet-connected businesses have relied upon periodic vulnerability assessments to manage their exposures to vulnerabilities. Annual or quarterly assessments are common. These assessments provide a "snapshot in time" – informing of known vulnerabilities affecting the

assessed systems. These snapshots have ever decreasing relevance over time, as the validity of the information expires rapidly with the release of new vulnerabilities.

This is not an assignment for an Intrusion Detection System

Intrusion Detection Systems (IDS) have their role in a layered security deployment where the use of IDS is deemed necessary. An IDS provides warnings when systems or networks are under attack. However, the IDS will not indicate whether or not the system or network is vulnerable to the attack.

Whether or not the organization deems it necessary to use an IDS does not provide any relief from the proper management of vulnerability exposures. Rapid knowledge of new vulnerabilities, combined with a responsive patch management strategy, enables the organization to protect their systems and networks before attacks originate. For example, enterprises who successfully patched their systems from the Slammer and Blaster worms prior to the attack had the luxury of ignoring the warnings set off by their IDS when the attacks originated, as they knew they were protected.

How Catbird Intelligent Vulnerability Monitoring works

Catbird Networks has taken a unique approach to vulnerability assessments. Instead of providing point-in-time snapshots, Catbird provides continuous IVM for external, Internet exposed networks, and internal, behind the firewall networks.

Catbird is the only solution in the industry that continually watches a customer's network while also monitoring the vulnerability advisories. If the monitored network changes, an alert is immediately sent. If a new vulnerability is released, a targeted assessment is immediately performed. IVM provides internal and external protection to keep networks locked down every day of the year.

Catbird's IVM solution watches both port status and the potential vulnerabilities in open ports. If a new port opens, not only is an alert sent, a targeted vulnerability scan immediately informs of any vulnerabilities on this new open port.

IVM is 24/7/365 – every day, around the clock, continuous protection. It starts with a complete vulnerability assessment as the initial "Kick-off", or baseline scan. A complete vulnerability report is generated, informing the user of all open ports, and of all known vulnerabilities and their severity. Once approved by the customer, this information is stored in the Catbird database and becomes the baseline against which all future monitoring will be compared.

There are two major differences between IVM and periodic assessments:

- Continuous monitoring of the customer's network for changes;
- Continuous monitoring of additions to the vulnerability database, where customers are automatically assessed for exposure to these new vulnerabilities.

If a port is found open that was closed in the baseline, the Catbird IVM system immediately notifies the customer. A vulnerability assessment is then automatically performed on just that newly opened port; and a targeted vulnerability report is sent to the customer with the specific results. If a port is found to be closed that was open in the baseline, the system immediately notifies the customer.

The vulnerability database is updated many times a day. As mentioned previously, there are currently over 300 new vulnerabilities being added each month. As new vulnerabilities are loaded, customers are automatically and immediately scanned. If nothing is found, neither report nor notification is sent. If something was found, an immediate, encrypted, vulnerability report is sent.

IVM happens every day, continuously. This is augmented by complete vulnerability assessments performed on a quarterly basis, enabling customers to use this for management, audit and examination documentation.

Conclusion: Catbird's IVM manages information to protect against vulnerabilities

Catbird's IVM watches for changes in a customer's network or changes in the vulnerabilities that may affect that network. The key to making use of this data is to have the right information sent to the right person at the right time.

Multiple reporting options are supported to track customer system vulnerability exposures, making it easy to gauge their status – without having to wonder if it is a false alarm or without being burdened by many pages of test results.

When new ports are opened or closed, or when new vulnerabilities are detected, the customer is informed immediately via email, cell phone or pager. When a new vulnerability is detected, the email message is accompanied by an encrypted report with the results of the targeted assessment, including information on how to fix the vulnerable system.

There are two levels of scheduled reports to provide information to operations managers and senior managers. Each contains the information critical to that specific audience. Operations Reports are specifically designed for the IT manager responsible for the daily management of IT security. Management Reports are high-level summaries, designed to convey important trend information to senior managers. Both Operations Reports and Management Reports can be sent automatically, or generated on demand.

The end result: Catbird's IVM gives customers 24/7/365 protection of their networks and systems against vulnerabilities. Catbird customers sleep well at night, knowing their businesses are protected.

---

[1] Internet week.com; December 29, 2003

[2] CERT - Testimony of Richard D. Pethia; Director, CERT® Coordination Center; Software Engineering Institute; Carnegie Mellon University; Pittsburgh, PA 15213; Before the House Committee on Government Reform; Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census Hearing on Worm and Virus Defense: How Can We Protect the Nation's Computers From These Threats?

[3] CNET news.com July 30, 2003)